

UNITED STATES DISTRICT COURT

for the

Southern District of Indiana

SEALED

United States of America

v.

Case No.

1:20-mj-0167

ANDREW SCOTT WHITAKER, JR.

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of unknown to & including 1/12/2020 in the county of Marion in the  
Southern District of Indiana, the defendant(s) violated:

Code Section

Offense Description

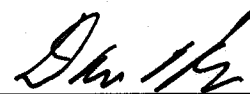
18 U.S.C. § 2252(a)(1)

Child Pornography Trafficking

This criminal complaint is based on these facts:

See attached Affidavit.

☒ Continued on the attached sheet.



Complainant's signature

Darin Odier, TFO/FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/21/2020



Judge's signature

City and state: Indianapolis, IN

Hon. Tim A. Baker, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT**

I, Darin Odier, being duly sworn, hereby depose and state as follows:

1. **Affiant:** I am a Detective in the Cybercrime Unit of the Indianapolis Metropolitan Police Department (IMPD). I am also a cross-designated Task Force officer assigned to the FBI's Indianapolis Violent Crimes Against Children Task Force.

2. **Experience:** I have over 30 years of law enforcement experience. I have investigated State and Federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have written numerous search warrants involving internet crimes against children cases and participated in their execution.

3. **Training:** I have attended and presented at the National Crimes Against Children Conference multiple times and attended numerous classes related to investigating the online sexual exploitation of children. I am also a member of the Indiana Internet Crimes Against Children Task Force, which includes federal, state, and local law enforcement agencies. I am currently assigned to operate in an undercover capacity on the internet to identify and investigate persons attempting to exploit or solicit sexual acts with children or trafficking in child pornography. As a Task Force Officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

4. **Information provided:** The statements in this affidavit are based on information obtained from my observations and communications, as well as

information learned from other law enforcement officers and witnesses. Because this affidavit is being submitted for the limited purpose of securing an arrest warrant and criminal complaint, I have not included each and every fact known to the investigators concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that **Andrew Scott Whitaker, Jr. (Whitaker)** committed a criminal offense.

5. **Probable Cause:** For the reasons listed below, there is probable cause to believe that **Andrew Scott Whitaker, Jr. (Whitaker)**, DOB XX/XX/19\*\* (known to affiant, but redacted) has committed the following offense in the Southern District of Indiana and elsewhere: **Count 1: Child Pornography Trafficking.**

6. **Child Pornography Trafficking: 18 U.S.C. § 2252(a)(1):** This investigation concerns alleged violations of 18 U.S.C. § 2252(a)(1), which prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

7. **Definitions:** The following definitions apply to this Affidavit:

8. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

9. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

10. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

11. **MEGA:** This is a cloud storage and file hosting service offered by Mega Limited, an Auckland, New Zealand-based company. The service is offered primarily through web-based apps. Mega mobile apps are also available for Windows Phone, Android and iOS. Mega is known for its security feature where all files are end-to-end encrypted locally before they are uploaded. This prevents anyone (including employees of Mega Limited) from accessing the files without knowledge of the pass key used for encryption.(Wikipedia)

12. **DROPBOX:** This is a file hosting service operated by American company Dropbox, Inc., headquartered in San Francisco, California, that offers cloud storage, file synchronization, personal cloud, and client software. Dropbox allows users to create a special folder on their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which device is used to view it. Files placed in this folder are also

accessible via the Dropbox website and mobile apps. Dropbox uses a freemium business model, wherein users are offered a free account with a set storage size and paid subscriptions for accounts with more capacity.

13. **GOOGLE:** This is an American multinational technology company that specializes in Internet-related services and products, which include online advertising technologies, search engine, cloud computing, software, and hardware. It offers services designed for work and productivity (Google Docs, Google Sheets, and Google Slides), email (Gmail), scheduling and time management (Google Calendar), cloud storage (Google Drive), instant messaging and video chat (Duo, Hangouts), language translation (Google Translate), mapping and navigation (Google Maps, Waze, Google Earth, Street View), video sharing (YouTube), note-taking (Google Keep), and photo organizing and editing (Google Photos). (Wikipedia)

14. **IMEI NUMBERS:** Every mobile device that connects to a cellular network has a unique International Mobile Equipment Identity number or IMEI number. This includes cell phones, smartphones, cellular-enabled tablets and smartwatches, and other devices that support cellular data. The IMEI number uniquely identifies a mobile device. It is separate from the SIM card or UICC number which is linked to a removable card in the device. This means the IMEI can be used to track or locate a specific device, regardless of what card is installed in it. For example, if your phone is stolen and the SIM card is swapped out, your mobile provider can still block access from the stolen phone using the IMEI.

15. An IMEI is similar to a serial number since it is a unique number linked to a hardware device. While serial numbers are generated by the manufacturer, IMEI numbers are produced by the GSMA (Groupe Spéciale Mobile Association), an international organization that oversees mobile network operators. The GSMA provides each mobile device manufacturer with a range of numbers to use for IMEIs on devices they produce. Manufacturers can choose their own convention for serial numbers, including the length and type of characters (numeric or alphanumeric). IMEI numbers are always 15 digits long, comprised of a 14-digit unique number followed by a "check digit" (or a checksum), which validates the number. (Techterms.com)

**Present Investigation and Overview of Specific Probable Cause:**

16. In October, 2019, this affiant, FBI Task Force Officer Darin Odier of the Indianapolis Metropolitan Police Department and Indiana ICAC Task Force received CyberTip number 49589714 from the National Center for Missing and Exploited Children (NCMEC), who alerts law enforcement to reports of sexual exploitation of children on the Internet. NCMEC was established in 1984 as a private, nonprofit 501(c)(3) organization. NCMEC provides services nationwide to families and professionals relating to preventing the abduction and sexual exploitation of children. Pursuant to its mission and congressional authorization (see 42 U.S.C. § 5773), NCMEC operates the CyberTip line and the Child Victim Identification Program to provide assistance to law enforcement in its efforts to identify victims of child pornography and child sexual exploitation.

17. NCMEC also works with law enforcement, Electronic Service Providers, electronic payment service providers and others in their efforts to reduce the distribution of child sexual exploitation images and videos on the Internet. NCMEC does not investigate and cannot verify the accuracy of information it receives. NCMEC forwards reports of possible child sexual exploitation to law enforcement for its independent review and analysis. This affiant has investigated numerous CyberTips from the National Center for Missing and Exploited Children.

18. After reviewing the CyberTip #49589714 submitted to NCMEC from Tumblr, Inc., this affiant observed a video of a showing multiple minor females with their vaginal areas exposed. Through my training and experience, I know this video constitutes child pornography under State and Federal statutes. The IP addresses for the logins listed in the cybertip geo-locate to the Indianapolis area.

19. The CyberTip provided the following information for the Tumblr, Inc. account being reported: Email address: ruohkanne@gmail.com, log-in or username: freetacohumanmaker, and/or Profile URL: freetacohumanmaker.tumblr.com.

20. This affiant knows that email addresses and specifically Goggle accounts frequently contain identifying information, photos, and/or other accounts that can assist in the identity of the account user.

21. This affiant requested and received a search warrant for Google, Google+ Photos, and Gmail account of ruohkanne@gmail.com and the above

requested items. The warrant was issued by Marion County Magistrate Jason Reyome on November 20, 2019.

22. The Google return showed multiple emails in the account inbox from Dropbox regarding a Dropbox, Inc. account with email address ruohkanne@gmail.com.

23. This affiant knows that Dropbox, Inc. accounts frequently contain identifying information in photos, documents and other media that can assist in the identity of the account user.

24. This affiant also knows from experience that collectors of child pornography and individuals sexually attracted to children often use Dropbox, Inc. to store and maintain their collections "in the cloud" instead of directly on their digital devices to prevent their discovery.

25. This affiant requested and received a search warrant for the Dropbox account with associated email address ruohkanne@gmail.com. The warrant was issued by Marion County Magistrate Ian Stewart on December 4, 2019.

26. The Dropbox search warrant return contained hundreds of images and videos this affiant believe constitute child pornography under state and federal statutes. The images and videos were categorized in multiple folders and sub-folders.

27. Included in the Google and Dropbox returns were IP logins. This affiant submitted a subpoena to Comcast for subscriber information of a specific IP address of 2601:807:8700:4220:e4ed:4a0b:fc1e:e3fb from October 11, 2019 at 07:45:02 UTC, as listed in the Google return for ruohkanne@gmail.com. The



same IP address is used to log into the Dropbox account associated with email address ruohkanne@gmail.com on October 11, 2019 at 07:33:27.

28. The return from Comcast for this IP address at the specific date and time of the log in noted shows the following information:

Subscriber name: JW (known to affiant, but redacted)

Service address: 5215 W. Henry St., Indianapolis, IN 46214

29. A BMV search shows JW (redacted but known to affiant), W/M, DOB XX/XX/19\*\* (known to this affiant but redacted) with an address of 5215 W. Henry St., Indianapolis, IN 46241. Also associated with the address is Andrew Whitaker, W/M DOB 04/01/19\*\* (known to affiant, but redacted).

30. Based on the above information, this affiant requested and was granted a search warrant for the residence located at 5215 W. Henry St., Indianapolis, IN 46214. The search warrant was issued out of Marion Superior court by Magistrate Travis Sandifur on January 14, 2020.

31. On January 16, 2020, this affiant and assisting officers executed the search warrant at 5215 W. Henry St., Indianapolis, IN 46241.

32. Among the occupants in the residence was Andrew Scott Whitaker, Jr. (Whitaker). This affiant read Whitaker his Miranda warnings which he acknowledged understanding. A multi part interview of Whitaker was recorded with audio and video.

33. During the search of the residence, officers learned that the middle room of the residence was a living room converted into a bedroom that Whitaker shared with his brother, JW (known to affiant, but redacted). Whitaker stated

he sleeps on the bed on the left side of the room as you enter from the kitchen and that his cell phone is on his bed.

34. A Samsung cell phone, model SM-A600TI with a Script R on the back was found on Whitaker's bed and seized pursuant to the search warrant. Whitaker provided a passcode for the cell phone and stated that no one, including his brother, knew his passcode. Whitaker stated that he has had multiple phones over the last few years and has been in possession of his current cell phone for 2-3 weeks, but has only been able to use it for approximately the past week. The phone has no assigned phone number and Whitaker uses it with Wi-Fi only to access the internet.

35. Whitaker stated he previously had a cell number of 317-742-4389 but that he gave it to his brother, JW, in March/April 2019. JW has since replaced that cell phone and ported the phone number to his new device. This affiant knows this phone number corresponds to the phone number on the Google subscriber information in the previous warrant return of ruohkanne@gmail.com. The account was created on June 21, 2018.

36. Whitaker denied using or being familiar with email addresses ruohkanne@gmail.com or Momsbakery333@gmail.com

37. Detective Jim Wailes, a forensic examiner with the IMPD Digital Forensics Unit was on scene and forensically examined Whitaker's cell phone pursuant to the search warrant. The passcode provided by Whitaker unlocked the cell phone and Det. Wailes was able to see that the IMEI number for the device is 359482090199073.

38. Det. Wailes was able to determine that 9 separate Google accounts, including Ruohkanne@gmail.com and Momsbakery333@gmail.com have been added to the device. When this affiant presented this information to Whitaker and asked him about it, Whitaker stated he wanted to speak with an attorney. This affiant then ended the interview. The nine google accounts are:

**Garyhost68@gmail.com**

**Slinkygirl27@gmail.com**

**Adox015@gmail.com**

**Lust4kime@gmail.com**

**Anneruohk@gmail.com**

**Taylorjim666@gmail.com**

**Ruohkanne@gmail.com**

**Momsbakery333@gmail.com**

**Lilk3154@gmail.com**

39. Det. Wailes noted that one of the Google accounts added to the phone, lilk3154@gmail.com, is associated with a Dropbox account. Det. Wailes was able to see the names of some of the files/folders accessed from the Dropbox account on the phone. They contained words such as PTHC and CP. Through my training and experience, I know that PTHC and CP are slang abbreviations for Pre-teen hard core and Child Pornography. Det. Wailes could visually see some thumbnail images from the Dropbox account and believes the thumbnails contain images of child pornography.

40. Det. Wailes also noted that Whitaker's Samsung phone contained

the MEGA app with a profile name of lil3154 and has an associated email address of lil3154@gmail.com. This affiant knows the Mega app is often used by collectors and distributors of child pornography. Files are shared among users through links that can contain hundreds of files.

**Attribution evidence that Whitaker controls the Google accounts:**

41. On January 17, 2020, this affiant applied for and received search warrants for the 9 Google accounts that had been added to Whitaker's cell phone. The search warrants were issued by Marion County Superior Court Magistrate Ronnie Huerta.

42. The Google returns included historical data showing that all devices that had been logged into these accounts by IMEI. This affiant reviewed the IMEI data for each of the Google accounts above and noted that a total of 14 separate devices have logged into these 9 Google accounts.

43. Based on the IMEI, this affiant knows that Samsung phone recovered from Whitakers' bed has been used to log into each of the 9 accounts.

44. The Goggle returns also show IP addresses used to log into the accounts. 7 of the 9 accounts have used the same IP address of 2601:807:8700:4220:e4ed:4a0b:fc1e:e3fb to log in since January 1, 2020. This is the same IP address used to log into the Dropbox account associated with Ruohkanne@gmail.com referenced above (Para 26).

45. 4 of the 9 accounts have used duplicate IP addresses to log in since January 1, 2020.

46. This affiant requested on IP subpoena for multiple IP's used by the 9 accounts. The subpoena return from Comcast shows the following IP addresses all returning to the residence at 5215 W. Henry St., Indianapolis, IN, where Whitaker resides.

2020/01/06-01:25:37-UTC | 2601:807:8700:810:a08f:8d1c:d7c4:9595

2020/01/06-22:30:36-UTC | 2601:400:109:af3a:5183:75ec:e468:7d45

2019/12/11-05:40:30-UTC | 2601:807:8700:810:a1a4:5ae9:e170:c421

47. The IP addresses were used to login to the Google accounts of lil3154@gmail.com, adox015@gmail.com and lust4kime@gmail.com, respectively.

48. The subpoena return from Comcast shows the following IP addresses all returning to the residence at 701 Manhattan Ave., Indianapolis, IN Indianapolis, IN and subscriber name AB (known to affiant, but redacted).

2020/01/12-10:07:53-UTC|2601:807:8700:2290:194f:104e:393e:386d

2020/01/12-10:35:05-UTC 2601:807:8700:2290:194f:104e:393e:386d

2020/01/12-16:35:33-TC|2601:807:8700:2290:194f:104e:393e:386d

49. The IP addresses were used to login to the Google accounts of momsbakery333@gmail, Lil3154@gmail.com and Ruohkanne@gmail.com, respectively.

50. On January 30, 2020, this affiant went to 5215 W. Henry St. and met with CB (known to affiant, but redacted), the mother of Whitaker. She identified AB (known to affiant, but redacted), as her sister and Whitaker's aunt. CB stated that Whitaker often stays at AB's residence.

51. This affiant reviewed the inboxes of the nine email accounts (Google accounts) and found multiple instances of overlap.

52. A January 12, 2020 email to Lilk3154@gmail.com from Dropbox.com reads, "Ann Ester (anneruohk@gmail.com) invited you to CP(1)". The email contains a folder with the name "CP(1)" and shows the size of the folder as 4.01GB.

53. Another January 12, 2020 email to Lilk3154@gmail.com from Dropbox reads, "alan key (ruohkanne@gmail.com) invited you to Neuer Ordner". The email contains a folder with the name "Neuer Ordner" and shows the size of the folder as 25.84GB. This affiant recognizes the folder name from the December 2019 Dropbox search warrant return for ruohkanne@gmail.com and has reviewed the folder and know it contains hundreds of images and videos of child pornography and child erotica. The size of the folder is 25.8GB and contains 5218 files.

54. The google photos folder for adox015@gmail.com contains a video of a male that this affiant recognizes as Whitaker.

55. On Sept 13, 2018 Taylorjim666@gmail.com received an email from Facebook addressed to "Andrew Popscott Whiaker", with a subject line Re:Robotface. This affiant found an active Facebook page for "Andrew Scott (Popscott)" that contain pictures of a person this affiant recognizes as Whitaker.

56. During the January 16, 2020 interview, Whitaker told this affiant that he plays bass guitar in a band named Robotface.

57. Several of the Google accounts have some of the other Google accounts listed in their contacts list.

58. The account Lust4kim@gmail.com has a search for "CP" in the search history. CP is known to this affiant to be slang and/or an abbreviation for Child Pornography.

59. The inbox for slinkygirl27@gmail.com shows an email dated January 2, 2020 from service@paypal.com with a subject line that reads "This money request has been cancelled" with a transaction ID of U-9JH75234NL467554N. This affiant requested and received a search warrant to PayPal Holdings, Inc. ("PayPal") for any accounts associated with email address slinkygirl27@gmail. The search warrant return from Paypal Holdings, Inc. lists the registration name on the account to be Whitaker. The phone number on the account is 317-742-4389. According to Whitaker, this was his phone number in January 2019 when the PayPal account was created.

60. There have been 3 credit cards associated with the PayPal account, all in the name of Whitaker. This includes an active card with the last 4 digits of 9290.

61. **Additional Dropbox warrants:** On January 18, 2020 this affiant requested and received search warrants for Dropbox, Inc. ("Dropbox") accounts associated with the 9 Google accounts. The search warrant returns show Dropbox accounts associated with 8 of the 9 email addresses, excluding taylorjim666@gmail.com.

62. Of the eight Dropbox accounts, seven contain images and/or videos of child pornography. Several of the accounts have folders with names suggestive of Child Pornography such as CP, CP2, xxx young, and real young pics 1. Several of the accounts contain some the same folders and files, but none of the accounts are not duplicates of each other.

63. The records contained in the return show multiple instances of folder sharing between the accounts.

64. The only Dropbox account not to contain child pornography has associated email address Garyhost68@gmail.com. The single folder in this account is entitled "2019 Robotface" and contains 10 audio files. As stated above, Robotface is the name of Whitaker's band.

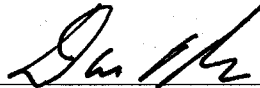
65. The Dropbox account for Anneruohk@gmail.com contains a folder entitled "Popscott's mixtape" and contains audio files of music. The name Popscott is consistent with the email from Facebook to Andrew "Popscott" Whitaker referenced above and located in the inbox of Taylorjim666@gmail.com. This Dropbox account also contains an image of Whitaker holding a bass guitar on a stage. A drum set with a Script R on the bass drum is visible in the image. This affiant recognizes the Script R from the back of Whitaker's cell phone.

66. The Dropbox returns included IP addresses used to log into the Dropbox accounts. A subpoena was issued to the internet service provider and listed 3 IP addresses, dates and time. The subpoena return showed 2 IP's were from Whitaker's residence 5215 W. Henry St. and the 3<sup>rd</sup> IP returned to AB's prior residence.



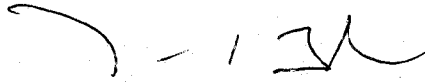
67. Based on the above information, this affiant believes that Whitaker has control of the Google and Dropbox accounts listed in this affidavit and uses these accounts to manage, share and control his collection of child pornography.

68. **Conclusion.** Based upon the contents of this Affidavit, there is probable cause to believe that Andrew Scott Whitaker, Jr. has committed the above- listed offense. I respectfully request that the Court issue a Criminal Complaint and Arrest Warrant for Andrew Scott Whitaker, Jr. charging him with the offense listed above.



Task Force Officer Darin Odier  
Federal Bureau of Investigation

Subscribed and sworn before me this 21st day of February, 2020.



Hon. Tim A. Baker  
United States Magistrate Judge  
Southern District of Indiana